ADS-B spoofing and mitigating measures

SAFE SKIES.
SUSTAINABLE FUTURE.

ICAO

Ho Wee Sin

Deputy Director (Air Traffic Management)
Civil Aviation Authority of Singapore

Presentation overview

01 Quick overview on ADS-B

02 Spoofing of ADS-B

03 Reasonableness checks on position

04 Other works by the aviation community

Quick overview on ADS-B

Automatic Dependent Surveillance-Broadcast

- Automatic - Does not require pilot intervention

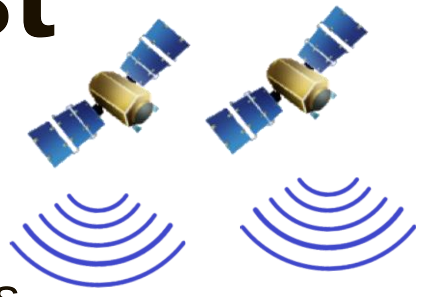
- Dependent - Require cooperation from the aircraft e.g. need aircraft to report information accurately

- Surveillance - Provide info on GNSS position, identity, altitude etc

- Broadcast - Information is broadcasted to receivers in range

ICAO

Automatic Dependent Surveillance-Broadcast



GNSS signals

Aircraft broadcasts GNSS position; Flight ID; Altitude; velocity etc

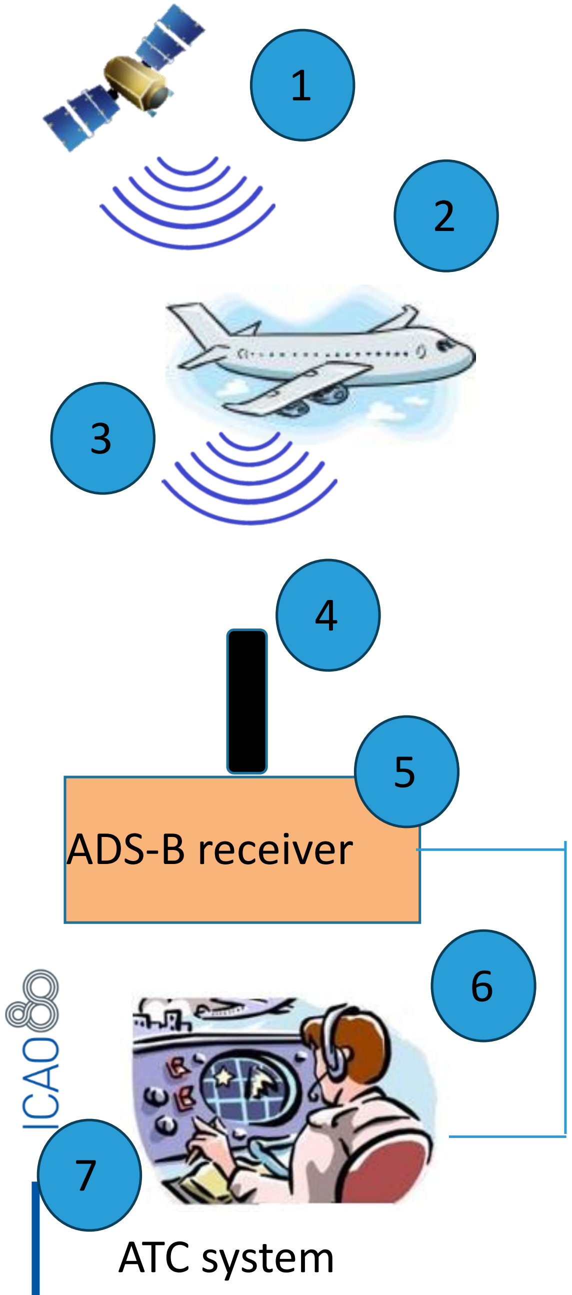
ATM system process info and display aircraft position to controllers. This information used for aircraft separation.

ADS-B receiver consolidates and processes information.

ADS-B receiver

Consolidated information transmitted to ATM system via comms lines.

Steps of ADS-B messages creation



1. GNSS satellites broadcast GNSS signals.

2. GNSS signals are received by GNSS antenna on aircraft. Aircraft equipment calculates position.

3. Aircraft transponder generates the ADS-B messages (including flight ID, velocity, altitude etc) and broadcast the ADS-B messages.

4. ADS-B messages are received by ADS-B receivers on the ground.

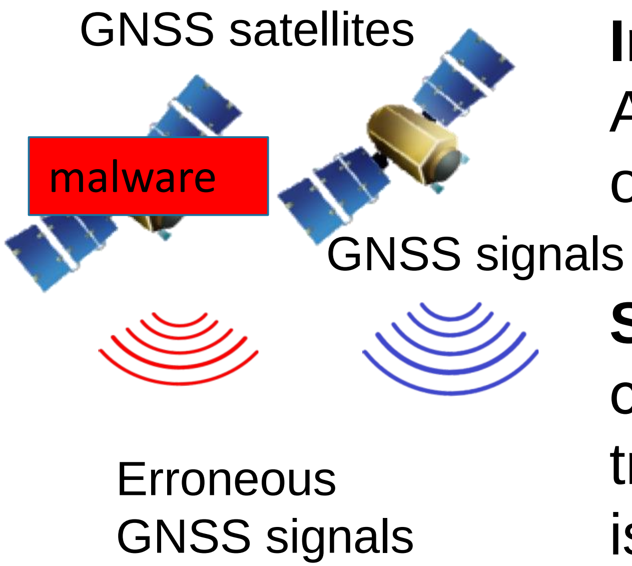
5. The ADS-B receivers compiles the ADS-B messages into ADS-B reports in ASTERIX CAT 21.

6. The ADS-B reports get relayed to the ATC system.

7. The ATC system processes the ADS-B reports and display as “aircraft position” to controllers.

Spoofing on ADS-B

Broadcasting of GNSS signals by GNSS satellites



Threat: Threat actor uploads malware to the GNSS satellites, causing it to provide wrong signals to users.

Impact: Multiple aircraft within a wide area will be affected. Erroneous ADS-B positions or ADS-B positions with poor accuracy indicators. Likely only affect one GNSS at a time.

Symptoms: Deviation of ADS-B tracks from radar tracks on the controller's display (in the case of erroneous ADS-B positions). Loss of tracks (in the case of poor indicators). Several ANSPs facing same issues. Area affected will be very large.

Means of detection: Anti-spoofing algorithms at receiver / ATM system.

Preventions: Security at the GNSS facilities.

Ops continuation: Use of alternatives (e.g. use only radars, wide area M-LAT or procedural control) over large area, possibly by several ANSPs.

Reception of GNSS signals by aircraft antenna

Threat: Threat actors may generate false GNSS signals that mislead the aircraft navigation systems. GNSS signals may also be jammed.

Impact: Aircraft within a smaller area will be affected. Erroneous ADS-B positions or ADS-B positions with poor indicators.

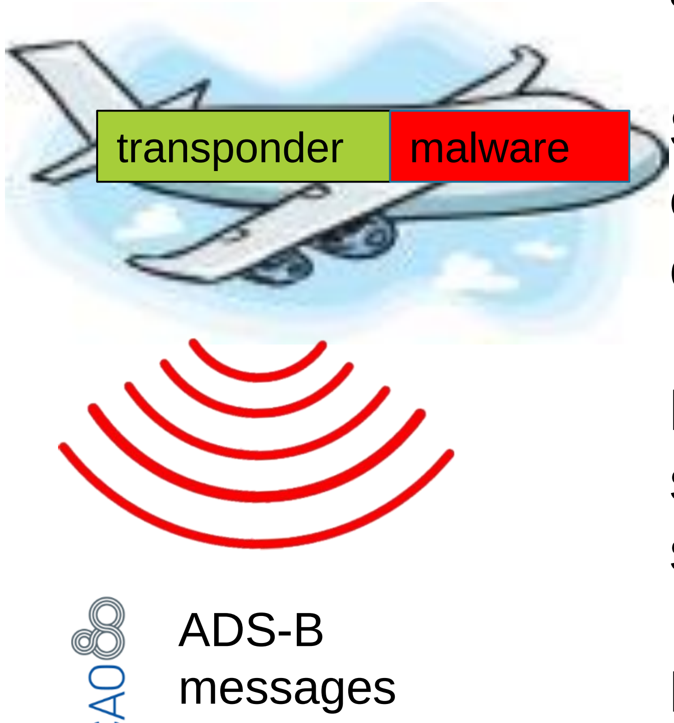
Symptoms: Deviation of ADS-B tracks from radar tracks on the controller’s display (in the case of erroneous ADS-B positions). Loss of tracks (in the case of poor indicators). Adjacent ANSP may experience same issues.

Means of detection: Anti-spoofing algorithm at receiver / ATM system.

Preventions: Import control of devices capable of spoofing GNSS signals. (difficult to enforce, especially oceanic or exterior territory)

Ops continuation: Use of alternatives over affected area.

Broadcasting of ADS-B messages by aircraft transponder



Threat: Malware may be installed onto the aircraft's transponder to generate misleading ADS-B messages.

Impact: Normally only one aircraft will be affected and that aircraft will show wrong position.

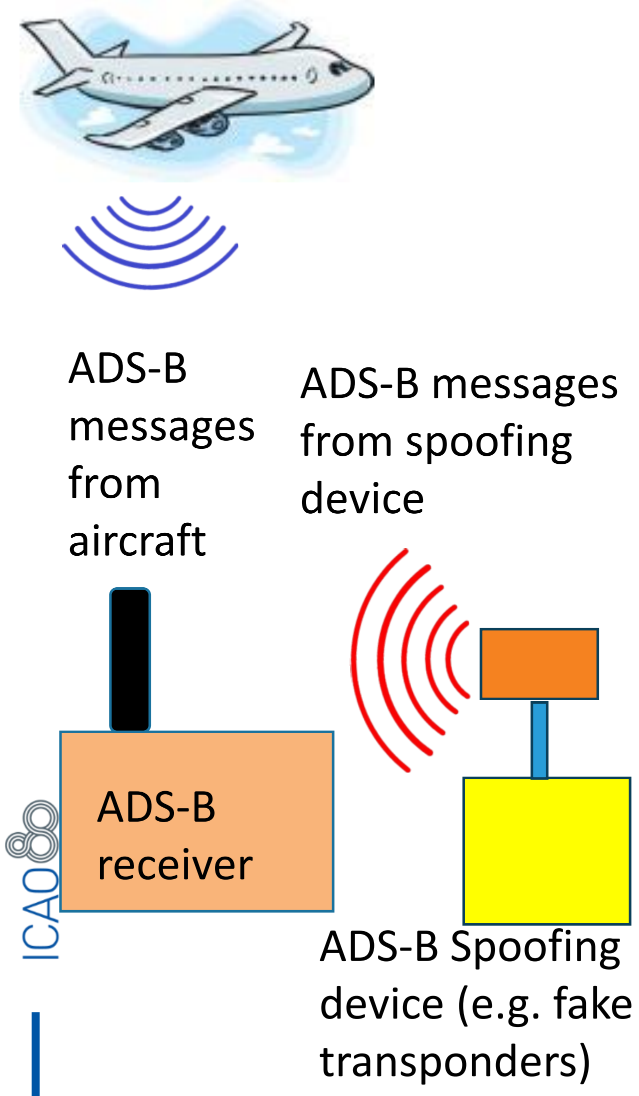
Symptoms: Deviation of ADS-B tracks from radar tracks on the controller's display (in the case of erroneous ADS-B positions). The other ANSPs will observe same error from that aircraft.

Means of detection: Anti-spoofing algorithms at receiver / ATM system. Route adherence monitoring alerts at ATM automation system.

Preventions: Security at aircraft maintenance facilities. Security within supply chain.

Ops continuation: Treat aircraft as a non-ADS-B equipped aircraft.

Reception of ADS-B messages by ADS-B receiver



Threat: Threat actors may set up transponders to broadcast fake ADS-B messages.

Impact: The ADS-B receivers with the range of the spoofing device will be affected.

Symptoms: “Additional” or “duplicate” aircraft will appear to the controller.

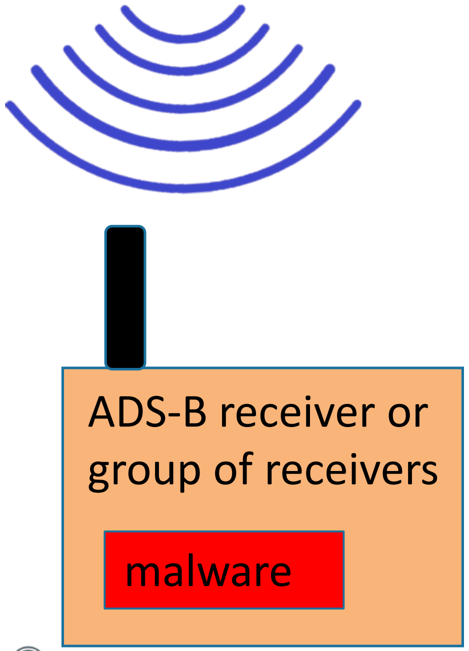
Means of detection: Anti-spoofing algorithm at receiver / ATM system. Check against flight plans. Request for pilot acknowledgement.

Preventions: Import control of devices capable of spoofing GNSS signals. (difficult to enforce, especially oceanic or exterior territory).

Ops continuation: Shut down / disconnect affected ADS-B receivers and rely on alternative surveillance sources.

Generation of ADS-B reports by ADS-B receiver

ADS-B messages from aircraft



Erroneous ADS-B reports being generated

Threat: Threat actors may install malware at the ADS-B receiver such that the receiver generates false ADS-B reports.

Impact: The affected ADS-B receivers will provide erroneous ADS-B reports to the ATM automation system.

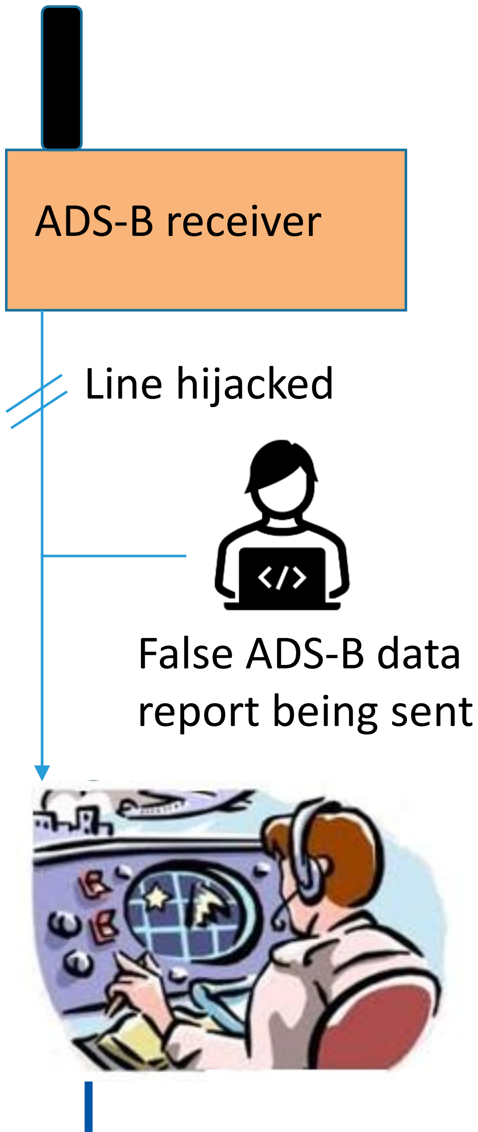
Symptoms: Dependent on the malware. Could include false targets, targets with wrong positions etc.

Means of detection: Deviation of ADS-B tracks from radar tracks on the controller's display. Checks against flight plans. Request for pilot acknowledgement.

Preventions: Security at the facilities. Security within supply chain.

Ops continuation: Shut down / disconnect affected ADS-B receivers and rely on alternative surveillance sources.

Transmission of ADS-B reports to ATM automation system



Threat: Threat actors may hijack landlines and inputs false ADS-B reports.

Impact: Erroneous ADS-B reports will be sent to the ATM system.

Symptoms: Could include false targets, wrong positions etc.

Means of detection: Deviation of ADS-B tracks from radar tracks on the controller’s display. Checks against flight plans. Request for pilot acknowledgement.

Preventions: Security at the facilities. Use lines that are less prone to hijacking (e.g. fibre optics). Transmit data via redundant paths.

Ops continuation: Shut down / disconnect affected lines. Make use of alternative network.

Display of Aircraft position on ATM automation system

Threat: Threat actors may install malware at the ATM automation system to display fake aircraft positions.

Impact: ATM automation system displays erroneous information to controllers.

Symptoms: "dependent on the malware".

Means of detection: Information from pilot does not match air situational picture. Air situation does not look normal.

Preventions: Security at the ATM facilities. Security within supply chain.

Ops continuation: Activate back-up system / sites.

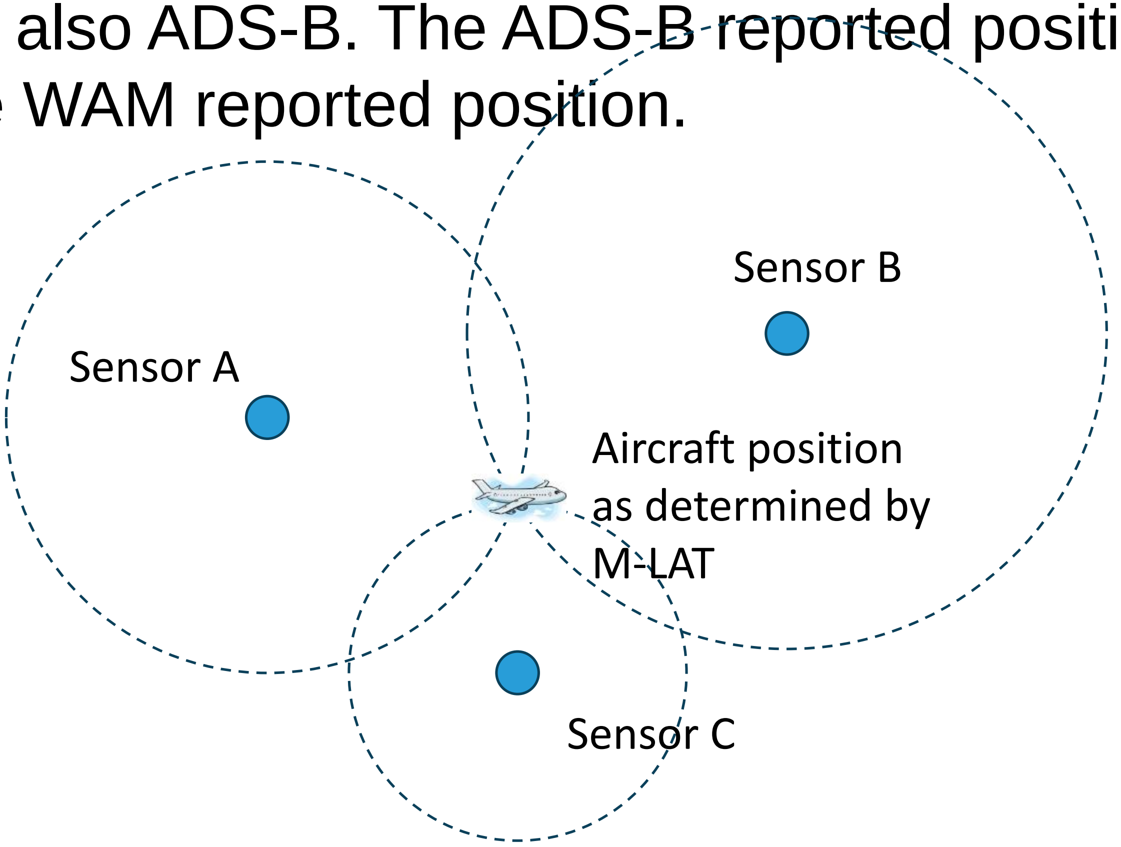
ICAO

Reasonableness check

Reasonableness check using Wide-Area Multilateration

Wide Area Multi-Lateration (WAM) System comprises of a network of sensors that can triangulate the position of target using time difference of arrival (TDOA).

These sensors are also ADS-B. The ADS-B reported position can easily be verified against the WAM reported position.

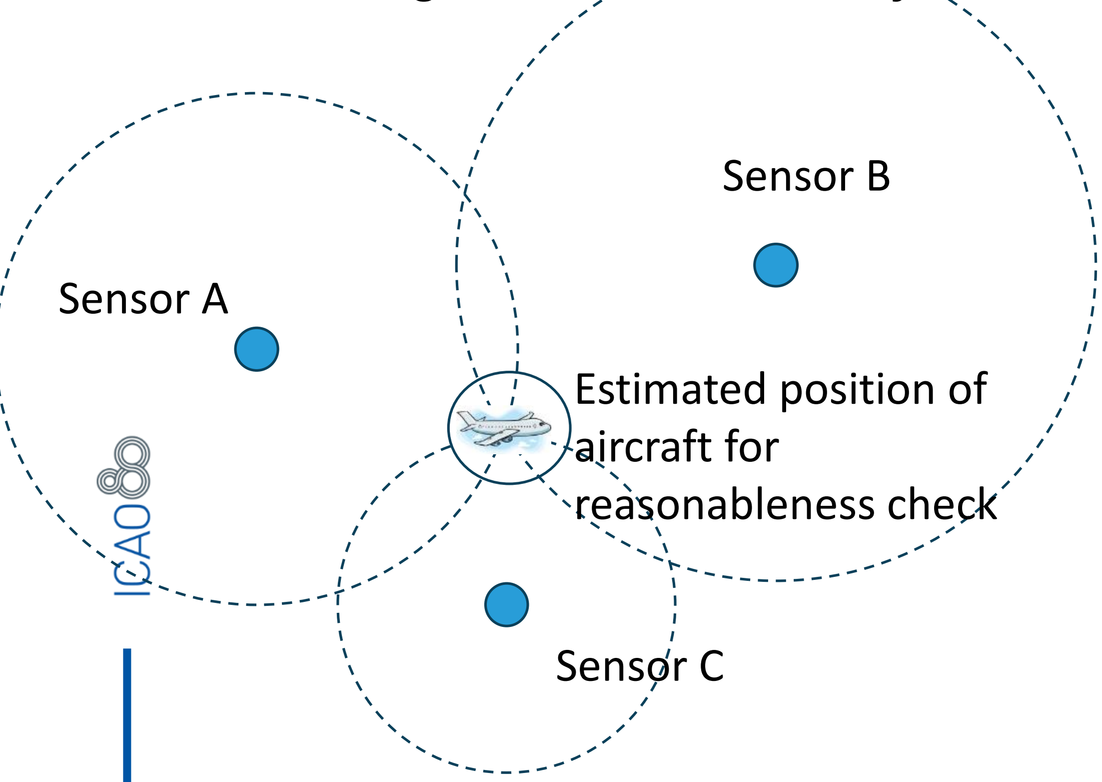


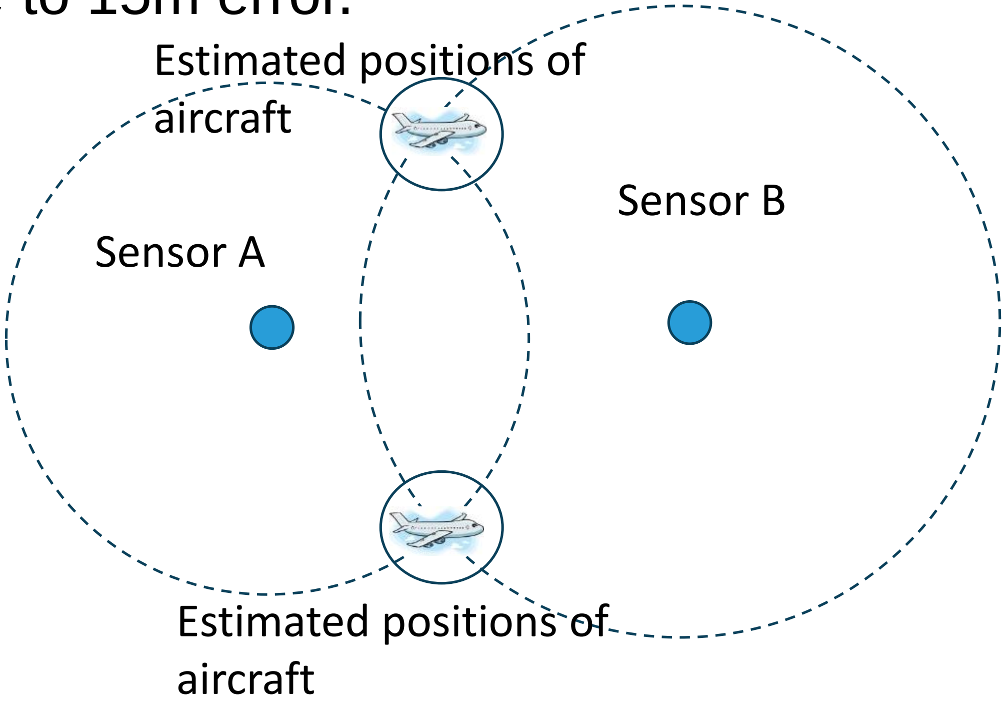
ICAO

Reasonableness check using a network of ADS-B receivers from the same manufacturer

With at least two ADS-B sensors with time stamp of high enough precision (e.g. I21/074 of ASTERIX CAT 21), it is possible to estimate the position of the target by triangulation, therefore performing a reasonableness check.

Sensors from same manufacturer are preferred as they are likely time-stamped using the same algorithm. Inaccuracy of 50ns will translate to 15m error.



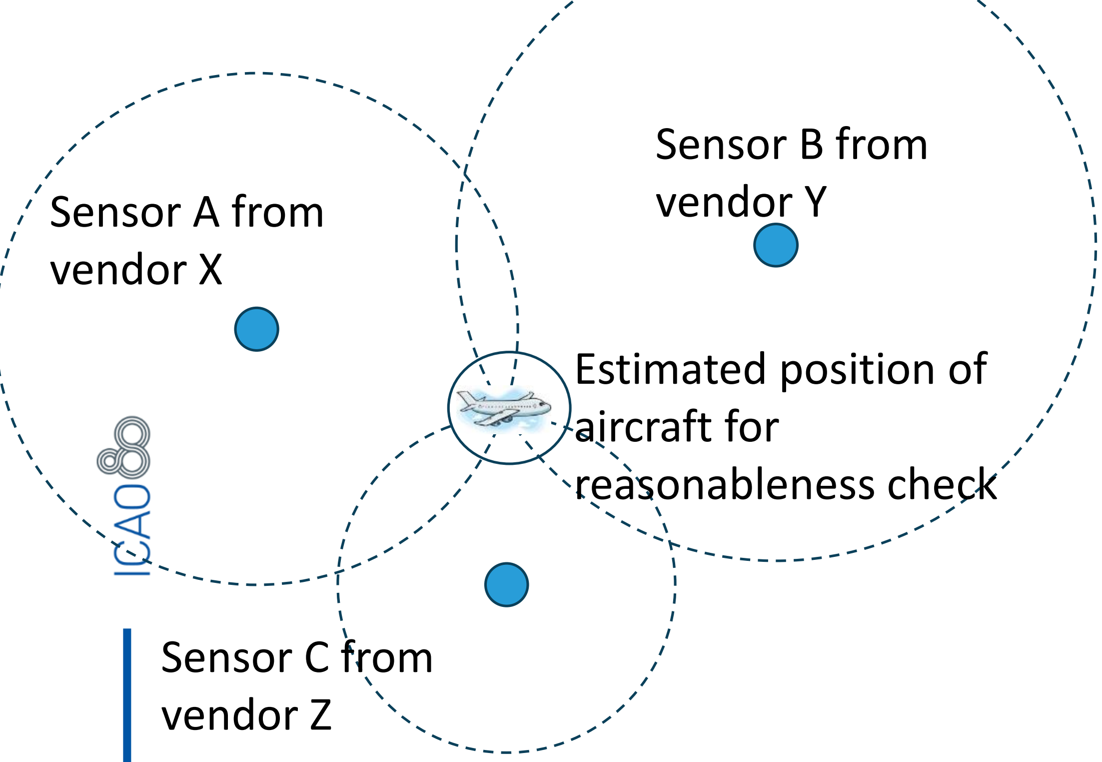


Reasonableness check using a network of ADS-B receivers from the different manufacturer

ADS-B receivers from different manufacturers are likely to time-stamp the message at slightly different points after detection of the signal.

Difference in time-stamping can be as great as 40μs, which translates to 12,000m of error.

It is possible to apply a correction in the time-stamp within the TDOA algorithm to reduce the error to 10μs. This will translate to an error of 3,000m (or 1.6nm).



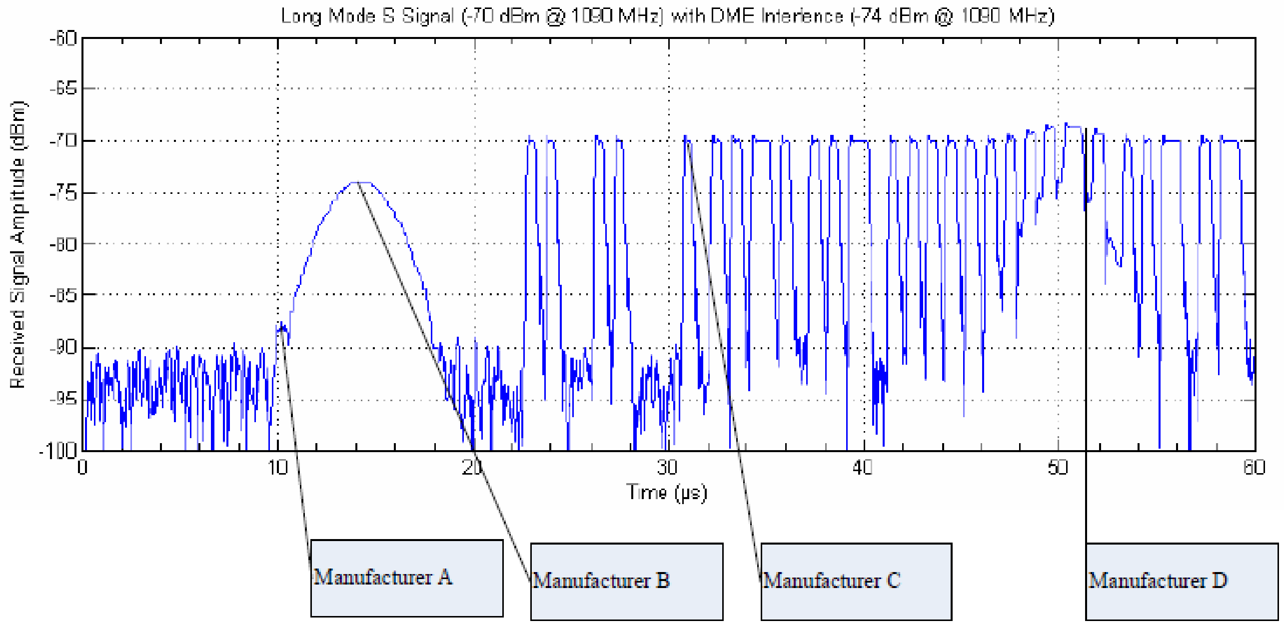


Diagram obtain from SURICG/4-IP15 by China

Other works by the aviation community

Detection of GNSS RFI by aircraft

- Capability to detect GNSS RFI is introduced in the new ED-259A and ED-259B MOPS.

- The GNSS RFI status information is proposed to be passed to the ground via ADS-B messages using two bits.
  - One for L1 and one for L5.

- The MOPS for the next generation ADS-B (version 3) was already finalized without considering GNSS RFI status information.

- Investigation is on going to explore incorporating GNSS RFI status information into ADS-B version 3 without introducing standardization challenges.

Detection of GNSS RFI using AI and ML

- Timely alert on GNSS RFI will be useful in the activation of appropriate contingency plans.

- Artificial Intelligence and Machine Learning can be employed to develop tools to detect spoofing or interference based on ADS-B messaged received on a real time basis.

- Organisations or States with large amount of ADS-B data can consider developing such tools.

Thank You

ICAO80